

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

-----x
UNITED STATES OF AMERICA,

v.
KEITH RANIERE,
Defendant.

Case No. 1:18-cr-00204-NGG-VMS

-----x
MEMORANDUM OF LAW IN REPLY TO
THE GOVERNMENT'S OPPOSITION TO
THE DEFENDANT'S NON-STATUTORY
MOTION TO COMPEL POST-JUDGMENT
MATERIAL & EXCULPATORY
DISCOVERY

In this reply, the Defense solely addresses the government's opposition (ECF No. 1213) regarding our Non-Statutory Motion To Compel Post-Judgment Material & Exculpatory Discovery (ECF No. 1192). A separate reply is forthcoming regarding the government's Rule 33 opposition.

The Motion To Compel was filed separately from, and never combined with, the Rule 33. The government chose, with the Court's approval, to provide an omnibus response. Further, treating the motion to compel before and separate from the Rule 33 issues is necessary here, due to a fairness issue created by the government's actions. The government, deeming it necessary for their opposition, granted their expert access to the forensic copies of the camera card (1B15a), which they continue to withhold from the Defense. The government's expert, FBI Senior Computer Scientist David Loveall II used these withheld items to make critical factual claims about the camera card in his declaration, responding to the seven Defense Experts' findings that photos were staged on the camera card, with manipulated metadata, based on their analysis of the metadata provided by the FBI. The government then included Loveall's declaration as an exhibit in their opposition. Thus, to competently reply to the government's Rule 33 opposition, the Defense must be given equal access to examine these still withheld items. Without access to these items, the Defense is blocked from verifying or refuting Loveall's critical factual claims.

Further, the government did not contest the *Brady* issues raised in our motion to compel, which established that these same exculpatory items be disclosed. Therefore, given the November 30, 2023 deadline for the Defense's reply, we respectfully request that the Court first compel the government to immediately disclose the requested evidence — specifically the FBI's two forensic copies of the camera card (1B15a) (NYC024299.001, the Flatley April 11, 2019 camera card copy and NYC024299_1B15a.E01, the Booth June 11, 2019 camera card copy), along with their corresponding log files — as outlined in the attached proposed order, using protocols designed by former FBI Special Agent and Forensic Examiner Dr. Richard Kiper to lessen the risk of further government tampering. (Exhibit A.)

Standards of fairness govern post-trial production. The law is clear. “[T]he very same principle of elemental fairness that dictates pre-trial production of all potentially exculpatory evidence dictates post-trial production of this infinitely narrower category of evidence.” *Dist. Attorney’s Office for the Third Judicial District v. Osborne*, 577 U.S. 52, 96 (2009); *see also, Bell v. Pool*, E.D.N.Y. April 10, 2003 00-CV-5214 (ARR) (The prosecution suppresses material exculpatory evidence in violation of *Brady* when it has possession or knowledge of such evidence and fails to disclose it to the Defense). The evidence to be disclosed here is both material and exculpatory — and falls well within the standard of elemental fairness.

This exculpatory evidence is material. The camera card was the purported source of the alleged child pornography on the hard drive. Its data tied Mr. Raniere to the alleged child pornography on the hard drive and to a particular Canon camera (1B15), whose foreign manufacture, they argued, established interstate commerce as the basis for federal jurisdiction. (Trial T. at 5372:14-23.) Without these links, the government would have lacked jurisdiction to

prosecute charges which, by their own admission, were “at the heart” of their case. (3/18/19 Pre-Trial T. at 19:15.)

The camera card is certainly exculpatory. This is proven by the government’s confirmation that the camera card was altered in FBI custody and that they allowed an unidentified, unauthorized “photo technician” to break the chain of custody and alter this item before it was preserved. (ECF No. 1213 at 11, n.6; Loveall Decl., ECF 1213-3 at ¶ 3.) Furthermore, the camera card was extensively falsified, according to the analysis of seven independent digital forensic experts, including four former FBI examiners. (Doc. 1169-1 at Bates 194-252; Dkt. 1192 at Bates 14-199.) Thus, there is a reasonable and strong likelihood that it contains additional proof of forgery by government agents, which is, by its nature, exculpatory.

No reason exists to prevent disclosure. The government has no legitimate reason to withhold this evidence from the Defense. These items are not alleged to contain any contraband photos. Yet, the government persistently withheld this evidence from the Defense in discovery and, in doing so, appears to have misled the Court:

- On September 13, 2018, regarding the seized devices, the government assured the Court that they would disclose “full discovery copies” of “all the material in our possession” and that such disclosures would include “metadata.” (9/13/18 Pre Trial T. (E.D.N.Y.) (Garaufis, J.) at 6:18-21; 9/13/18 Pre-trial T. (E.D.N.Y.) (Scanlon, J.) at 5:21-6:6).
- On September 18, 2018, the government informed the Court that the devices were already being processed by the authorized unit, the Computer Analysis Response Team (CART), and that this process had begun “within days” of the search and seizure at 8 Hale. (9/18/18 Pre-Trial T. (E.D.N.Y.) (Scanlon, J.) at 37:4-12.) This was untrue. The devices from 8 Hale,

were delivered to CART 134 days after seizure, except for the camera and card, which had not yet been delivered to CART and would not be until 332 days after seizure. (DX 945)

- However, on September 19, 2018, the government directed an off-the-books operation, enabling an unidentified non-CART “photo technician” to access the camera card. The government’s excuse at present is that “law enforcement agents,” – who lack authority to direct the handling of digital evidence – allegedly deemed the metadata unimportant.¹ (ECF No. 1213, page 11, footnote 6.) The government claims that it was during this “photo technician’s” handling that the card was altered, an event that resulted in crucial data being erased forever.
- On September 25, 2018, the government disclosed merely a PDF printout of photos from the “photo technician’s” access of the camera card (created by the prosecution’s² Paralegal Specialist Teri Carby, not CART), in contrast to a full copy of the device, as they claimed they would do twelve days earlier on September 13. Importantly, the PDF that was provided omitted the valuable metadata at issue here, also in direct contradiction of the government’s assurance to the Court on September 13.
- On September 27, 2018, AUSA Tanya Hajjar asserted, “We just pulled out the pictures...**and gave them everything.**” (9/27/18 Pre-Trial T. at 35:6-9.) (emphasis added) However, this was not true. First, they did not provide a forensic copy of the camera card, which would have contained the crucial metadata at issue here. Second, their actions went beyond merely “pull[ing] out the pictures.” The PDF printout contained photos that were deleted on the card.

¹ In a sex trafficking case focused on photos termed ‘collateral,’ it is implausible that “law enforcement agents” truly believed evidence from the sole camera seized and alleged to be used by Mr. Raniere to be unimportant.

² FBI policy prohibits prosecuting attorneys from authorizing or having a role in the processing, analysis or reporting of original digital evidence. (Eldridge Report, ECF No. 1192 at Bates 26).

To recover them and make them visible required the “photo technician” to perform a forensic operation, which was unauthorized and undocumented.

- On March 18, 2022, the government also rebuffed our post-conviction informal request for this discovery and, adding to their series of misrepresentations, falsely stated that the government had fulfilled all discovery obligations prior to the jury trial in this case.
- On July 21, 2023, after concealing the off-the-books mishandling of the camera card from the Defense and the Court for more than four years, the government then buried this pivotal revelation in a footnote in its opposition to the Defense’s motion. (ECF No. 1213, page 11, n.6.)

Further proof of tampering has been indicated. Critical omissions in the government’s opposition strongly suggest discrepancies between the FBI’s two forensic copies of the original camera card, which could indicate further tampering while in FBI custody. For example, Loveall declared, “I have examined the disk images [forensic copies] created of 1B15 and 1B15a and determined that they are identical.” (Loveall Decl. at ¶ 9.) Notably, here, Loveall misidentifies the two different copies of the camera card (one created by Flatley on April 11, 2019, and one created by Booth on June 11, 2019), as the trial record and a prior assertion in Loveall’s declaration make clear that “1B15” is the camera and “1B15a” is the camera card. However, and more importantly, he provided *no proof* of these items being identical even though such proof would have been readily at hand given that Loveall had access to both copies of the camera card. Recall, the trial testimony of FBI Senior Forensic Examiner Brian Booth wherein he stated that in order to verify that different image copies are identical, the FBI relies on the “hash value” or digital fingerprint of each forensic copy. (Trial T. at 4784:2-22.) When dealing with potentially billions or trillions of bytes of data, the “hash value” is what allows a forensic examiner to

confirm that every single byte across two copies is an exact match. If even one byte is off, the copies cannot be said to be “identical.” An experienced examiner and scientist like Loveall making such a critical claim without also including basic, easy-to-obtain, and required hash values appears to be intentional, rather than an oversight. Thus, there is a strong logical inference that the two forensic copies are in actuality different since he chose to omit readily available data which is the required and expected proof for his crucial claim that the two withheld copies are identical. Given like access to copies of these two camera cards, it would take Defense experts very little time to compare the “hash values” of each and confirm whether they are identical with absolute, scientific certainty. If the hash values between Flatley’s April 11, 2019 copy of the camera card and Booth’s June 11, 2019 copy are found to be different, that would prove indisputably, irrefutably, and unquestionably that the camera card was maliciously tampered with while it was in FBI custody between April 11, 2019 and June 11, 2019, in the weeks before and/or during jury trial.

We must guard against further evidentiary tampering. Given the extensive proof of government involvement in this evidentiary malfeasance, and the government’s continued withholding of evidence that is likely to further implicate them, there is a risk that the government will attempt to circumvent a court order compelling them to disclose this evidence, namely by providing only a portion of the data or by providing the data in a manner that compromises its forensic integrity. Hence, we urge the Court to compel the government to follow Dr. Kiper’s proposed forensic protocol when producing the requested evidence to lessen the risks of further tampering or destruction. (Exhibit B., Kiper Declaration) This will not unduly burden the government as it primarily involves copying existing materials. In fact, the time spent by the government in opposing this justified disclosure is far more time than that required to simply

disclose the requested evidence. Finally, we implore the Court to order **immediate** disclosure, as delays increase further tampering risks, and since, given the Defense's reply to the government's Rule 33 opposition is due on November 30, 2023, our experts will need time to analyze this crucial evidence, *as was already afforded to the government's expert, Loveall*. To put it simply, the government filed an opposition where it included a rebuttal affidavit from its expert who relied upon and referenced the withheld copies of the camera card in its assertions. The Defense, in order to competently reply to the government's opposition, must now have our experts forensically examine these same items, which the government possesses and refuses to disclose. To deny this request by the Defense would be to deny basic fairness and obscure the full extent of the government's malfeasance.

Dated: October 23, 2023

Respectfully submitted,

/s/ Arthur L. Aidala
/s/ Michael Jaccarino
Aidala, Bertuna & Kamins, P.C.
546 5th Avenue, 6th Floor
New York, New York 10036
Attorneys for Keith Raniere

/s/ Joseph M. Tully
Tully & Weiss Attorneys at Law
713 Main Street
Martinez, California 94553
Attorney for Keith Raniere